

AFFIDAVIT

I, Todd F. Porinsky, your Affiant, being duly sworn, state that the following is true and correct to the best of my knowledge and belief, and is submitted in support of establishing probable cause to support the filing of criminal complaints against Honorio Herrera and Yasmany Cabello Morell, as more specifically set forth below.

1. Between on or about June 29, 2017, and on or about July 3, 2017, in the Northern District of Ohio, Honorio Herrera and Yasmany Cabello Morell, did knowingly commit and aid and abet the following criminal offenses against the United States, to wit: (1) knowingly and with intent to defraud, possess 15 or more access devices which were counterfeit or unauthorized, in violation of Title 18, United States Code, Section 1029(a)(3); (2) knowingly and with the intent to defraud, produced, possessed, trafficked in, and had custody and control of device making equipment (as defined in 18 U.S.C. Section 1029(e)(6)), in violation of Title 18, United States Code, Section 1029(a)(4); Aggravated Identity Theft, in violation of 18 United States Code, Section 1028A(a)(1); and aiding and abetting in violation of 18 United States Code, Section 2.

2. I am a Special Agent with the United States Secret Service ("USSS"), assigned to the Cleveland Field Office. I have been employed with the USSS as a special agent since September 2002. Prior to my employment with the USSS, I worked for two years as an Accounting Technician for the U.S. Department of Defense Finance Accounting Service. As part of my employment as a special agent with the USSS, I have received training in general law enforcement and criminal investigations at the Federal Law Enforcement Training Center and at the U.S. Secret Service Rowley Training Center, including training in the detection and investigation of violations of 18 U.S.C. § 1029, concerning fraud and related activity in connection with access devices. I have had training and experience in organized

crime investigations and money laundering investigations.

3. Through investigation, it has been determined that members of criminal organizations consisting primarily of individuals of Cuban decent have recently travelled to the Northern District of Ohio, and elsewhere, to commit access device fraud by illegally obtaining debit and credit card account information from gas station customers through the unauthorized placement of electronic devices known as “skimmers” inside gasoline pumps. One type of “skimmer” device attaches to the computer of the point-of-sale credit card reader, and is illicitly placed on gas station pumps. The skimmer device copies the electronically transmitted account information (i.e. full track data) found on the magnetic strip of an unsuspecting customer’s credit card, including the customer’s name, account number, zip code for the billing address on the account, and the card expiration date, which enables valid electronic payment authorization to occur between a merchant and the issuing financial institution. The stolen credit card account information and other data is accumulated and stored on the “skimmer,” and subsequently removed and downloaded onto a computer. With some of the more advanced skimmer devices, the stolen account information can be transmitted from the skimmer while installed on the gas pump to a suspect’s computer through “WiFi” or Bluetooth connections.

4. A second electronic device used in furtherance of schemes to steal and use debit and credit card account information is known as a credit card reader/writer/encoder. A credit card reader/writer/encoder is designed to provide a means to read and re-write the account information and other electronic data found on the magnetic strip on debit and credit cards. The device can read and write tracks 1, 2, and 3 of data from the magnetic strips, while simultaneously decoding, encoding, and verifying three tracks of data from the debit and credit cards. Examples of cards that can be read and re-written include debit and credit cards, as well as customer loyalty cards, gift cards, employee ID cards, and hotel room keys. These devices can also be used by an individual to re-encode customers’ debit and

credit card data onto a blank or counterfeit credit card.

5. A laptop is a mobile computer, typically the size of a notebook, that is mobile, battery operated and easily transported. Laptops can function as wireless communication devices and can be used to access the Internet through cellular networks or “WiFi” networks. Laptops typically contain software programs, the same as a personal computer, which perform different functions and save data associated with those functions. Programs can, for example, permit accessing the Internet, sending and receiving e-mail, and participating in programs which allow another user to remotely access the laptop from another geographic location via the Internet. For purposes of the scheme described herein, the laptop acts as the receiver of stolen credit card data from the “skimmer” device which is transmitted via a wireless signal. The laptop is subsequently used in conjunction with the credit card reader/writer/encoder to transfer the victims’ stolen debit and credit card information fraudulently obtained with the skimmer device, to a counterfeit or cloned credit card. The resulting cloned or counterfeit credit cards are then used by individuals to purchase merchandise, goods and services at various retailers, and to complete other types of financial transactions using the victims’ debit and credit card account information which had been re-encoded onto the magnetic strip of the counterfeit card.

6. On July 3, 2017, Brecksville Ohio Police Department Patrolman K. Ackerman was conducting speed enforcement activity on Interstate 77 when a Jeep Patriot passed him clocked at 88 m.p.h. in a 65 m.p.h. posted area. The vehicle was driven by Yasmany Cabello Morell and Honorio Herrera was seated in the front passenger seat. After being pulled over by Officer Ackerman, Morell and Herrera told Ackerman they were vacationing in Cleveland. Officer Ackerman noticed there was no luggage visible inside the vehicle. Officer Ackerman requested permission to search the vehicle, which consent was granted by Cabello Morell, the driver of the vehicle.

7. While conducting a search of the Jeep, officers discovered two gas pump “skimmer” cables under the front passenger floor mat. A backpack located on the rear passenger seat contained a Lenovo laptop computer and a MSRSX6 Magnetic Card Reader/Writer. Located in the center console was a wallet containing five reloadable MasterCard debit cards with the words “A GIFT FOR YOU” embossed on the front of the cards in the location where the accountholder’s name is normally embossed.

8. Brecksville Police Patrolman C. J. Wirkus transported the five reloadable MasterCards to the Brecksville Police Department to use a credit card reader to detect and read the data on the cards’ magnetic strips. The card reader showed that instead of data for a MasterCard reloadable debit card, the magnetic strips on each card contained the data for other individuals’ credit card accounts; the account numbers on the magnetic strips did not match the account numbers embossed on the front side of the cards. Your Affiant knows from training and experience the numbers embossed on the front of a MasterCard, and the number electronically encoded on the back of the card, should be the same. When the numbers do not match, it is indicative that the card is a counterfeit access device. Here, Officer Wirkus made the determination that the numbers on the front and the back of the cards in Cabello Morell and Herrera’s possession did not match and therefore the cards were counterfeit.

The information found on the cards was as follows

Name and Account on Magnetic Strip

BATISTE/STEPHEN A 5470315930970944

HOLLINGSWORTH/CATHLEEN 4717241001904412

ABELL/SARAH D 5145730700353409

PAINTER/ TRAVIS 4342562926375831

GAGE/BOBBY H 5424323677235759

Name and Account on Front of Card

A GIFT FOR YOU 5164889029628788

A GIFT FOR YOU 5164882387841879

A GIFT FOR YOU 5164883467368403

A GIFT FOR YOU 5164889089697897

A GIFT FOR YOU 5164883401141783

9. At that time, Cabello Morell and Herrera were arrested for state charges of Possession of Criminal Tools and transported to the Brecksville Police Department Jail. Twinsburg Police Department Patrolman Y. Encarnacion arrived at the jail and advised Cabello Morell and Herrera of their Miranda rights in Spanish. Herrera declined to be interviewed.

10. Later that morning, your Affiant arrived at the Brecksville Police Department. Brecksville Police Detective James Lobenthal and your Affiant transported Cabello Morell to the Twinsburg Police Department where Ptl. Encarnacion could translate Spanish to English for Cabello Morell. Cabello Morell waived his Miranda rights agreed to be interviewed by your Affiant, Det. Lobenthal and Ptl. Encarnacion. During the interview, Cabello Morell admitted to being involved in the credit card skimming at gas station pumps and to his involvement in credit card fraud. Cabello Morell said he and Herrera flew to Cleveland on June 29, 2017, and were given instructions by a man named Oscar. Cabello Morell said he did not know Oscar's last name. Oscar mailed a laptop to the WoodSprings Suites Hotel (20829 Emerald Parkway, Cleveland, Ohio), where Cabello Morell was staying. Upon arriving at the WoodSprings Suites Hotel, Cabello Morell took possession of the package containing the computer mailed by Oscar.

11. Cabello Morell said he drove to approximately four gas stations in northeast Ohio. By phone, Oscar gave Cabello Morell instructions concerning the location of gas stations to which Morell should drive. Cabello Morell told your Affiant that once near the gas stations, while sitting in the passenger seat of the vehicle, Herrera would turn on the computer sent by Oscar, and start a program that would enable the computer to be remotely controlled from Miami. Oscar told Herrera what to do over the telephone. Herrera typed a code into the computer, and as it was being remotely controlled by Oscar, the stolen customers' credit card

data was transferred from the “skimmer” device installed on the point of sale terminal installed inside the gas pump to the laptop computer via a Bluetooth wireless signal. Cabello Morell said that Oscar used that stolen account information and other data to make counterfeit credit cards in Miami.

12. Cabello Morell said someone else had placed the “skimmers” inside the gas pumps prior to Cabello Morell’s arrival in Cleveland. He stated that his and Herrera’s job was to drive around to the gas stations and download stolen credit card account information from skimmer devices until they flew home on July 7, 2017. Morell said they were given five counterfeit cards by Oscar to use for living expenses while traveling, and that he had also used the cards for retail purchases at Walmart stores in the Cleveland area. Cabello Morell said the more work he does for Oscar, the more he will get paid.

13. Also on the same date, your Affiant presented a Consent to Search Form written in Spanish to Cabello Morell. Ptl. Encarnacion provided additional explanation in Spanish concerning the consent form. Cabello Morell indicated his desire to cooperate and executed the form agreeing to allow authorities to search his WoodSpring Suites hotel room #407, the Lenovo computer, the additional computer equipment found in the vehicle, and his cellular phone for evidence related to the skimming activity and the credit card fraud scheme.

14. Brecksville Police Detective Frank Faulhaber and Detective C. Grimm travelled to Woodspring Suites, room 407, to conduct the consent search. Inside room 407, the detectives found Walmart receipts which corresponded to the time period described by Cabello Morell during his interview with Your Affiant; a copy of hotel payment for Yasmany Cabello dated June 30, 2017; an American Airlines boarding pass for Yasmany Cabello from Charlotte, North

Carolina to Cleveland, Ohio on June 29, 2017; and a credit card “skimmer” board. There was packaging for a MSRX6 Bluetooth Magstrip Card Reader and an opened U.S. Postal Service shipping box dated for delivery on July 1, 2017 to Yasmany Cabello at the WoodSpring Suites address. Three credit cards with the name Yasmany Cabello and Yasmany L. Cabello-Morell were also found in the hotel room.

15. While the Brecksville detectives were searching the WoodSpring Suites hotel room, our Affiant accessed Cabello Morell’s LG cell phone. The phone was not password protected and Cabello Morell had previously given written consent to search the phone. Your Affiant saw two numbers in the contact list for “Oscar.” Your Affiant opened the photo application on the phone. There were numerous photos of gas pumps, along with screenshots of gas station locations from a phone mapping application. Your Affiant recorded those screenshots and informed Brecksville Detective Lobenthal of the addresses of the stations in the screenshots on Cabello Morell’s phone. Detective Lobenthal directed other detectives to travel to those addresses to check the gas station pumps for “skimmers.” Your Affiant also found images in photo files in Morell’s phone of a laptop screen. There is a screenshot on the phone showing computer program “MSR Utility Program (for HD & Bluetooth) v3.0.” This is a program for reading/writing/encoding credit cards. Among items on the screen are command prompts “READ CARD”, “Please swipe card Swipe Counter 3” and boxes for Track 1, Track 2, and Track 3. In the box for Track 1 is the name ABELL/SARAH D and data for a credit card number account ending in 3409, and the Track 2 box contains the same credit card account number. Images were also found on Morell’s phone depicting a screenshot for the computer program “TeamViewer.” Commands on the screen show “Allow Remote Control”, “Control Remote

Computer” and “File Transfer.”

16. Later that day, Brecksville Detective C. Grimm and Lt. S.A. Korinek travelled to the Shell gas station, 1683 State Road, Cuyahoga Falls, Ohio. This was one of the addresses Your Affiant had provided to the Brecksville detectives from Morell’s phone. The station manager, Valerie Ann Reisig, told the detectives that she had been receiving messages via a smart phone application that some of the gas pumps had been malfunctioning since June 30, 2017. The Brecksville detectives opened all six pumps at the Shell station, noting that pumps #4 and #6 appeared to have been tampered based upon the appearance of the seal tape on the pump face. Upon opening the door to the gas pumps’ electronics, “skimmer” devices were found on both pump #4 and #6. Both “skimmers” were photographed, removed and sealed in evidence bags for transport by the Brecksville detectives.

17. On August 1, 2017, pursuant to the written consent to search the Lenovo computer signed by Morell, agents from the USSS conducted a forensic examination of the computer’s hard drive. A software program called “MSRX” was identified as being loaded on the computer. Your Affiant knows from training and experience, and from consultation with agents trained in the USSS Electronic Crimes Special Agent Program (ECSAP) that this software application is used in connection with the downloading of electronic data and other information from devices such as skimmers. Another program loaded on the computer is “TeamViewer.” This is a program used to remotely access the laptop from another geographic location via the Internet. Both programs found on the computer corroborate Morell’s verbal account of how the skimming scheme worked, and correspond to images found on his phone. The forensic examination of the Lenovo computer revealed that the software application had been used on

July 2, 2017, the day before Morell and Herrera were arrested in Brecksville, Ohio. Forensic examination further revealed that the computer's hard drive also contained approximately 370 stolen credit card account numbers along with the account holders' names, and other related information which appears to have been skimmed from customers' credit cards at point-of-sale terminals.

18. Based on the foregoing, I respectfully submit that there is probable cause to believe that between on or about June 29, 2017, and on or about July 3, 2017, in the Northern District of Ohio, Eastern Division, and elsewhere, Honorio Herrera and Yasmany Cabello Morell, committed and aided and abetted the commission of the following offenses against the United States:

Title 18, U.S.C., Sections 1029(a)(3) – knowingly and with the intent to defraud, possess 15 or more devices which are counterfeit or unauthorized access devices, such conduct effecting interstate or foreign commerce;

Title 18, U.S.C., Section 1029(a)(4) – knowingly and with the intent to defraud produce, possess, traffic in, and have control and custody of device-making equipment (as defined in 18 U.S.C., Section 1029(e)(6)) such conduct effecting interstate or foreign commerce; and

Title 18, U.S.C., Section 1028A(a)(1) – during and in relation to felony violations enumerated in 18 U.S.C., Section 1028A(c), to wit: 18 U.S.C., Sections 1029(a)(3) and 1029(a)(4), did knowingly transfer, possess and use, without lawful authority, the means of identification of another person (Aggravated Identity Theft).



Todd F. Porinsky
Special Agent, U.S. Secret Service

Sworn to before me and subscribed in my presence, this 02ND day of August, 2017, at
Cleveland, Ohio.


JONATHAN D. GREENBERG
United States Magistrate Judge